

**CLAIMS****We claim:**

1. A method for capturing one or more graphic primitives and attributes associated with such graphic primitives of a display object, the method comprising the 5 steps of:

injecting a spy component into a target process by a calling process, wherein the spy component is an executable program module;

capturing the one or more graphic primitives and attributes associated with such graphic primitives during the execution of the target process; and

10 returning the graphic primitives and attributes associated with such graphic primitives to the calling process.

2. The method of claim 1, wherein the step of injecting the spy component is performed by an injection component that is invoked by the calling process.

15

3. The method of claim 2, wherein the injection component is an executable program module comprising executable routines for injecting source code into a target process.

20

4. The method of claim 1, wherein the step of injecting includes inserting one or more function patches into one or more executable program modules that correspond to an operating system upon which the target process is being executed, the executable program modules having instructions for rendering graphics primitives to a graphical user interface.

25

5. The method of claim 4, wherein the step of inserting the function patches is performed by the spy component.

30

6. The method of claim 1, wherein the step of injecting includes installing one or more hook functions into the operating system APIs that generate system

messages in the event of a display object being output to a user interface screen during the execution of the target process.

7. The method of claim 6, wherein the step of installing is performed by the  
5 spy component.

8. The method of claim 6, wherein the system messages provide context information that is descriptive of an invoked action within the target process.

10 9. The method of claim 6, wherein the one or more hook functions are installed by a hook management component that is called upon by the spy component after injection into the target process.

15 10. The method of claim 9, wherein the hook management component is responsible for uninstalling the one or more hook functions upon termination of the target process.

20 11. The method of claim 1, wherein the step of capturing includes calling the one or more hook functions to intercept any system messages generated as a result of an invoked action within the target process.

12. The method of claim 11, wherein the one or more hook functions set a flag to activate the one or more function patches installed by the spy component.

25 13. The method of claim 1, wherein the step of capturing includes invalidating a display object that is output to a user interface as a result of the invoked action within the target process.

30 14. The method of claim 13, wherein the step of invalidating includes calling the function patches to capture the graphics primitives and attributes associated with such graphics primitives as they are drawn to the user interface to render the display object.

102016060000

15. The method of claim 1, wherein the step of returning includes sending the context information captured by the one or more hook functions to the calling process as a system message.

5

16. The method of claim 1, wherein the step of returning further includes sending the graphics primitives and attributes associated with such graphics primitives that are captured by the one or more function patches to the calling process as a system message.

10

17. A computer-readable medium having computer-executable instructions for capturing one or more graphic primitives and attributes associated with such graphic primitives of a display object, the computer-executable instructions performing steps comprising:

15        injecting a spy component into a target process by a calling process, wherein the spy component is an executable program module;  
              capturing the one or more graphic primitives and attributes associated with such graphic primitives during the execution of the target process; and  
              returning the graphic primitives and attributes associated with such graphic  
20        primitives to the calling process.

18. A system for capturing one or more graphic primitives and attributes associated with such graphic primitives of a display object, the system comprising:

25        an injection component for injecting a spy component into a target process  
              residing on a computer;  
              a spy component for capturing graphics primitives and attributes associated with such graphics primitives in connection with system messages that are generated by the target process as a result of an invoked action within the target process; and  
              a hook management component for installing and uninstalling one or more hook  
30        functions into one or more program modules that are executed by an operating system

SEARCHED  
INDEXED  
SERIALIZED  
FILED

residing on the computer, the program modules having instructions for generating system messages during the execution of the target process.

19. The system of claim 18, wherein the injection component is an executable  
5 program module consisting of executable instructions for injecting the spy component  
into the executable code of the target process.

20. The system of claim 18, wherein the injection component injects the spy component into the target process on behalf of a calling process.

10

21. The system of claim 20, wherein the calling process is a computer executable application.

22. The system of claim 18, wherein the spy component inserts one or more  
15 function patches into one or more executable program modules that correspond to the  
operating system upon which the target process is being executed, the executable  
program modules having instructions for rendering graphics primitives to a graphical user  
interface.

20

23. The system of claim 22, wherein the function patches capture graphics primitives and associated attributes of such graphics primitives that are rendered to a user interface by a display object as a result of an action invoked within the target process.

24. The system of claim 23, wherein the spy component packages the graphics primitives and attributes associated with such graphics primitives and sends it to the calling process as a system message.

25. The system of claim 18, wherein the spy component calls the hook management component to insert one or more hook functions into one or more executable program modules that correspond to the operating system upon which the target process is being executed, the executable program modules having instructions for

generating system messages in the event of a display object being output to a user interface during the execution of the target process.

26. The system of claim 25, wherein the one or more hook functions set a flag  
5 to activate the one or more function patches installed by the spy component.

27. The system of claim 25, wherein the one or more hook functions intercept any system messages generated as a result of an invoked action within the target process.

10 28. The method of claim 27, wherein the system messages contain context information that is descriptive of an invoked action within the target process.

29. The system of claim 18, wherein the spy component packages the context information and sends it to the calling process as an OS message.

15 30. The system of claim 18, wherein the hook management component is responsible for installing and uninstalling hook functions on behalf of the spy component.

20 31. The system of claim 30, wherein the hook functions are uninstalled by the hook management component upon termination of the target process.

TOP SECRET - SOURCE CODE